REMARKS

I.   Introduction

In response to the Office Action dated October 18, 2005, claims 11, 16, 26, 41, 46, and 56 have been cancelled, and claims 1, 15, 17, 30, 32, 45, and 47 have been amended. Claims 1-10, 12-15, 17-25, 27-40, 42-45, 47-55, and 57-59 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II.   Specification Amendments

Applicants' attorney has made amendments to the specification as indicated above. The amendments were to clarify the serial numbers for various cross-referenced cases. In addition, the amendments were submitted to overcome the objections to the drawings. The drawings have not been amended and the support for the amendments to the specification are clear from the drawings themselves.

In view of the above, Applicants respectfully request withdrawal of the objections to the specification.

III.   Non-Art Rejections

In paragraph (4) of the Office Action, claims 12, 13, 27, 28, 42, 43, 57, and 58 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. In paragraph (5) of the Office Action, claims 12, 13, 27, 28, 42, 43, 57, and 58 were rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. In paragraph (6) of the Office Action, claims 6, 17, 21, 32, 36, 47, and 51 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicants respectfully traverse the above rejections.

With respect to claims 12, 13, 27, 28, 42, 43, 57, and 58, the claims were rejected stating that while the specification suggests the use of multiplexors with the hardware state machine, nowhere is it described in the manner in which the multiplexors are actually used or configured. The rejections

-12-

further state that it is unclear how the multiplexors relate to the remainder of the invention.

Applicants refer the Patent Office to paragraphs [0070]-[0074] that provide as follows:

[0070]   The hardware state machine 718 may contain the same logic as used in the prior art and may not be modified. In addition to the state machine 718, the implementation consists of a permutation that employs a series of configurable multiplexors at the beginning 716 and end 720 of the fixed hardware state machine 718. Custom logic (i.e., the logic within hardware configuration control and IO module 714) interconnects the multiplexors (within permutations 716 and 720) to the system bus 612 of CAM 512. Accordingly, the hardware configuration control and IO module 714 that connects to the system bus 612 controls access to the permutation 716 and 720 and state machine 718 logic.

[0071]   The custom logic within the control and IO module 714 implements a key exchange protocol by accepting (or rejecting) a series of pre-authorized keys (e.g., sequentially wrapped keys with n=10^6 times or other large value) or other secure protocol. The key defines a configuration for the permutations 716 and 720. Valid keys are only known to the headend (e.g., uplink center 104) by using any public key algorithm such as Rabin or RSA (Rivest-Shamir-Adelman). Based on a public key algorithm, the keys cannot be recreated or generated by unknown parties. The keys are delivered to the smart card either over the broadcast stream, Internet, or other appropriate distribution channel. The keys can be delivered to the smart card (i.e., CAM 512) population asynchronously (e.g., over a period of several hours, days, or months). The keys may be delivered using uniquely encrypted, group encrypted packets. These packets are unintelligible to members (i.e., CAMs 512) for which they were not encrypted. In other words, the packets are only intelligible to those members/control and IO modules 714 having the appropriate private key.

[0072]   The hardware configuration control and IO module 714 verifies/authenticates the key. Such a verification/authentication may ensure that the key is from a known source (e.g., a known uplink center 104, program source 200A-200C,etc.), that the key is not a duplicate of an already received key, or that the key fails to comply with an additional security measure. As part of the authentication process, the control and IO module 714 decrypts the keys. The decrypted key is then verified/authenticated by the custom logic within module 714. If the key is valid, the key is retained by the control and IO module 714 (e.g., by storing the keys in protected registers with no physical or logical output mechanism outside the custom logic within the module 714). If the key is invalid, the key is rejected and may not be stored by the control and IO module 714.

[0073]   As described above, the key defines a configuration for the permutations 716 and 720. Accordingly, when appropriate, the key is used to dynamically (i.e., on-the-fly) reconfigure the permutations 716 and 720. The timing of the reconfiguration may occur immediately upon receipt of the key. Alternatively, the key may be stored by control and IO module 714 and only used to reconfigure the permutations 716 and 720 (e.g., switch the configuration to that represented by the stored key) upon receipt of an over the air command. In such a circumstance, the control and IO module 714 may store a currently active key (that defines a permutation 716 and 720 currently being used) and a future key. Accordingly, the

-13-

keys may be delivered asynchronously over a very long period of time to multiple CAMs 512 where they are validated and stored asynchronously. Thereafter (e.g., once a period of time has passed to ensure that appropriate/enough CAMs 512 have the new key), an over the air command to activate a reconfiguration operation for a key may be delivered synchronously to all CAMs 512. Thus, the actual reconfiguration operation may occur simultaneously within all CAMs 512, while the key delivery and validation mechanism is asynchronous over a period of time. [0074] To recongifure the permutations, 716 and 720, the control and IO module 714 communicates bi-directly 722 with the pre-permutations 716 and post-permutations 720 to dynamically configure the series of multiplexors in each respective permutation 716 and 720. Once configured, the pre-permutations 716 place the digital services information received across communication link 724 from control and IO module 714 into the appropriate form for use by the hardware state machine 718. Hardware state machine 718 may modify the digital services information based on custom logic within the state machine 718. Thereafter, the post-permutations 720 may modify the outgoing digital services information to limit use and viewing of the information from unauthorized attackers.

The *The American Heritage® Dictionary of the English Language, Fourth Edition Copyright © 2000* (see www.dictionary.com) defines permutation as "A rearrangement of the elements of a set." Further, a multiplexor is merely a hardware device having one or more inputs and one or more outputs where the mulitplexor determines the signal that is output. As set forth in the specification above, the control and IO module 714 communicates with the permutations to dynamically configure the series of multiplexors in each permutation. The specification further provides, that once configured, the pre-permutation places the digital services received from the control and IO module 714 into the appropriate form for the hardware state machine 718. Thereafter, the post-permutation modifies the outgoing digital services information to limit the use and viewing of the information from unauthorized attackers (see paragraph [0074]). Thus, the specification clearly describes the manner in which the multiplexors are configured and used within/by permutations. In addition, as set forth in the specification, the keys that define the configuration are used to dynamically reconfigure the permutations (and the multiplexors within the permutations). Further, since the multiplexors are employed by the permutations and are configurable, the specification clearly supports and enables the use of such multiplexors to one with knowledge in the field of art.

The Office Action rejects claims 17, 32, and 47 based on the phrase "or other distribution channel". Applicants disagree and traverse the lack of disclosure of "or other distribution channel". In this regard, Applicants refer to paragraphs [0015], [0028], [0033], [0071], and [0076].

-14-

Nonetheless, in the interest of expediting prosecution, Applicants have amended the claims to remove the objectionable language.

The Office Action rejects claims 6, 21, 36, and 51 in that it is unclear what the terms uniquely encrypted, group encrypted" encompasses. Applicants refer the Patent Office to paragraph [0071] of the specification that includes the following language:

> ...The keys can be delivered to the smart card (i.e., CAM 512) population asynchronously (e.g., over a period of several hours, days, or months). The keys may be delivered using uniquely encrypted, group encrypted packets. These packets are unintelligible to members (i.e., CAMs 512) for which they were not encrypted. In other words, the packets are only intelligible to those members/control and IO modules 714 having the appropriate private key.

As can be seen from the claims, the configuration information is encrypted (see claim 3). The encrypted configuration information is uniquely encrypted. As described in paragraph [0071], such unique encryption means that the packets are unintelligible to members (i.e., CAMS 512) for which they were not encrypted. Each CAM has an appropriate key as described. Therefore, the key is uniquely encrypted for each CAM. Further, the configuration information is encrypted in a group of packets. Such language, intent, and meaning is clear from the express/explicit language of the claims and is supported in the specification.

IV. Prior Art Rejections

In paragraph (7) of the Office Action, claims 1-12, 14-27, 29-42, 44-57, and 59 were rejected under 35 U.S.C. §102(b) as being anticipated by Wasilewski et al. (Wasilewski), U.S. Patent No. 6,157,719. In paragraph (8) of the Office Action, claims 13, 28, 43, and 58 were rejected under 35 U.S.C. §103(a) as being unpatentable over Wasilewski, in view of Killian, U.S. Patent No. 5,222,141.

Specifically, independent claims 1, 15, 30, and 45 were rejected as follows:

> As to claims 15, 30, and 45, Wasilewski discloses an access system for set-top boxes wherein configuration information may be transmitted to the set-top box as a one-time event (i.e. asynchronously). Since the set-op box's function is to determine whether an encrypted instance should be decrypted, it constitutes a security component that controls access to digital services. The received configuration information (the EMM) comprises decryption keys (control words) to be implemented (see column 6, line 24 to column 7, line 24) in a hardware state machine (the DHCT) such as an ASIC (see column 15, lines 32-36 and figures 2B and 3).

> As to claim 1, a control suite (the control center) sends transmissions via satellite, which inherently employs an uplink center for sending transmissions to the satellite. The stream is incorporated at a media server for distribution (see column 15, lines 7-24).

Applicant traverses the above rejections for one or more of the following reasons:

-15-

(1)   Neither Wasilewski nor Killian teach, disclose or suggest the dynamic reconfiguration of a hardware state machine within a CAM/smart card; and

(2)   Neither Wasilewski nor Killian teach, disclose or suggest a hardware state machine within a CAM/smart card that is not directly accessible to a system input/output module or system bus of the CAM/smart card.

Independent claims 1, 15, 30, and 45 are generally directed to the use of a CAM/smart card to prevent unauthorized access to digital services. Specifically, configuration information for accessing digital services are transmitted asynchronously to a subscriber. The CAM/smart card receives the configuration information. The CAM/smart card has many components including a custom logic block and a hardware state machine. The amended claims provide that the hardware state machine is not directly accessible to a system input/output module or system bus of the CAM/smart card. Further, the custom logic block is configured to dynamically reconfigure the hardware state machine based on the configuration information that is received. Also, it is noted that the hardware state machine comprises custom logic that is used to control access to the digital services.

Thus, as claimed, since the hardware state machine is not accessible to the system input/output module or system bus of the CAM/smart card, and because the implementation is hardware based, it is protected from being altered by the microprocessor of the CAM/smart card or external means.

In the prior art, hardware was not reconfigurable as claimed. Further, the prior art failed to protect the integrity of the CAM/smart card. In this regard, tin the prior art, software within the CAM/smart card was merely altered through inappropriate manipulation of the microprocessor memory access control unit. However, in the present invention, not only is hardware used, but the hardware is isolated from/not accessible to a system input/output module or system bus (and thereby not directly accessible to the microprocessor).

The Office Action rejected independent claims 1, 15, 30, and 45 based on Wasilewski. With respect to the hardware state machine, the Office Action merely relied on Wasilewski's use of an ASIC referring to col. 15, lines 32-36 and figures 2B and 3. In addition, original dependent claims 11, 14, 26, 29, 41, 44, 56, and 59 (of which some of the dependencies have been incorporated into the independent claims) were also rejected based on Wasilewski's use of a DHCTSE. These

-16-

rejections assert that the components of the DHCTSE communicate with one another via a local bus (relying on Figure 12 and column 21, lines 15-27). FIG. 12 provides:
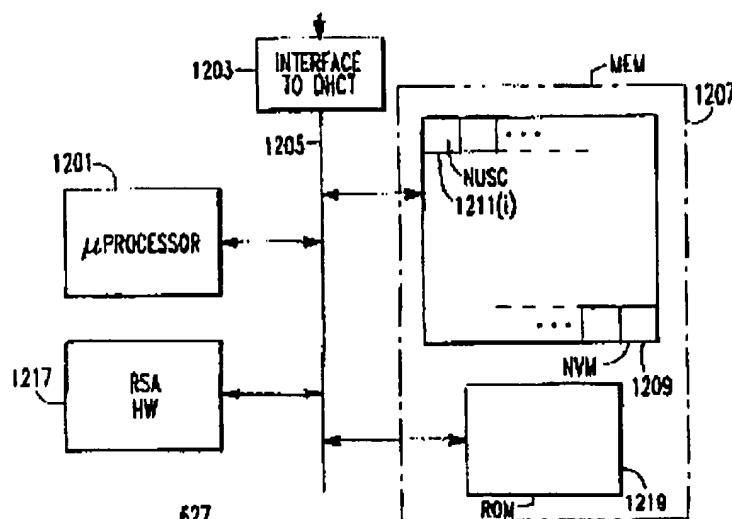
FIG. 12

As can be clearly seen in FIG. 12, all of the components within the DHCTSE are connected to the local system bus. The Office Action admits such a connection. However, the claims provide that the hardware state machine within the CAM/smart card is not directly accessible to the bus of the CAM/smart card. As can be seen, while the interface to the DHCT 1203 provides an interface to the DHCT, all of the components within the DHCTSE are accessible to the bus 1205 of the DHCTSE. Thus, rather than isolating or limiting access of the various components (as claimed), Wasilewski explicitly describes and provides that the various components are all accessible via the bus of the CAM/smart card.

The Office Action attempts to assert that the local bus is different than the system bus. Applicants submit that the claims explicitly provide that the system bus referred to is the system bus of the CAM and not of the set top box or DHCT. Thus, the local bus referred to in Wasilewski is the bus that is not directly accessible to the hardware state machine in the current claims.

In view of the above, Applicants submit that Wasilewski fails to teach, disclose, or suggest the invention as claimed. Further, Killian fails to overcome the deficiencies of Wasilewski.

-17-

Moreover, the various elements of Applicants' claimed invention together provide operational advantages over Wasilewski and Killian. In addition, Applicants' invention solves problems not recognized by Wasilewski and Killian.

Thus, Applicants submit that independent claims 1, 15, 30, and 45 are allowable over Wasilewski and Killian. Further, dependent claims 2-10, 12-14, 17-25, 27-29, 31-40, 42-44, 47-55, and 57-59 are submitted to be allowable over Wasilewski and Killian in the same manner, because they are dependent on independent claims 1, 15, 30, and 45, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-10, 12-14, 17-25, 27-29, 31-40, 42-44, 47-55, and 57-59 recite additional novel elements not shown by Wasilewski and Killian.

V.   Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

By: _____

Name: Georgann S. Grunebach, Reg. No. 33,179
Attorney for Applicants

Date: January 11, 2006

The DIRECTV Group, Inc.
RE / R11 / A109
P.O. Box 956
2250 E. Imperial Highway
El Segundo, CA 90245-0956

Phone: (310) 964-4615

-18-